

Applicant: Petteri Lannes et al.  
Application No.: 10/598,392  
Response to Office action mailed Jan. 11, 2008  
Response filed April 18, 2008

### Remarks

Claims 21–43 remain pending in the application. In the Office action dated Jan. 11, 2008, claims 21, 22, 24–25, 31–34, and 37 were objected to as containing informalities. Claims 22, 24, 26, and 28–32 were rejected as indefinite. Claim 21–22, 24, 26–27, 31, 33–39 and 41–43 were rejected as anticipated by Maki, and claim 23, 25, 28–30, and 32 were rejected as obvious over Maki in view of Hill, Jr. et al.

The claims have been amended to overcome the formalities and correct the indefiniteness identified by the examiner.

“Stateful” is a key limitation of the claims, and yet is somewhat difficult to comprehend, yet it does have a definite meaning to those skilled in the art. Apparently the term *stateful* was coined in 1993 by Check Point Software (the same year their patent US 5,606,668 on a stateful firewall was filed) as a description of a type of firewall see <http://www.checkpoint.com/press/1997/patent2.html>.

The meaning of *stateful* or *statefully* is: a way of looking at data, and making decisions, which is more than making decisions based only on administrator-defined rules (as in static analysis) but includes the context that has been established by prior packets that have been processed by the information system and thus relies upon a unique configuration of information in a program or machine. (See [http://www.webopedia.com/TERM/S/stateful\\_inspection.html](http://www.webopedia.com/TERM/S/stateful_inspection.html) attached.)

A stateful firewall is programmed to distinguish legitimate packets for different types of connections by allowing only packets matching a known connection state through the firewall. (See wikipedia: State (computer science), Stateful firewall, and [http://www.webopedia.com/TERM/S/stateful\\_inspection.html](http://www.webopedia.com/TERM/S/stateful_inspection.html) attached). In the context of the claimed invention this means that a control signal sent to the maintenance process is not based on a single parameter input but rather on a broader range of inputs including the values of other parameters including past states.

Thus applicants are claiming an off-site maintenance information system which directly takes action to control a maintenance process based, not on a single limit being

Applicant: Petteri Lannes et al.  
Application No.: 10/598,392  
Response to Office action mailed Jan. 11, 2008  
Response filed April 18, 2008

exceeded, but on the basis of the entity formed by: the condition monitoring system, the data-collecting unit, the message relay system and the teleservice center, so providing automatic instructions for actions, which traditionally have required active action by the service staff.

Maki (US Pub 2002/0052715) provides an off-site maintenance information system, which transmits data back to the Service System Server of the production plant. The Maki system is indicated as providing “Resultingly effective tools ... for processing fault information concerning a machine malfunction situation and issuing instructions to the production plant 20.” (See paragraph [0030] US Pub 2002/0052715.)

The difference as now claimed is that while Maki (US Pub 2002/0052715) implicitly requires personnel involved in controlling the maintenance process, the present invention explicitly does not, and more particularly, the claimed invention employs a data structure claimed as stateful, which is nowhere mentioned in the prior art applied by the examiner, nor has the examiner shown this type of data structure applied, to the claimed “maintenance of machines, processes, automation systems and equipment relating to papermaking”.

#### **Response to the examiner’s argument.**

Claim 21 is rejected as anticipated over Maki. Maki is a system for collecting and storing and organizing data, which can be used for personnel action or the action of outside suppliers. Maki paragraphs [0009] through [0012] set forth in the objects of the invention, which do not describe a system of taking action, but rather one of transferring, and storing data, and making data available through authorized parties. Maki Paragraph [0017] speaks of:

The novel communications connection by virtue of the invention between a papermaking production plant or the like and a service providing unit facilitates a plurality of *novel approaches to the implementation of maintenance and servicing activities*. For instance, continuous data collection from the operation of a production plant *gives enhanced possibilities of anticipating future needs of servicing*. In certain situations, *the scheduled maintenance periods may be extended*

Applicant: Petteri Lannes et al.  
Application No.: 10/598,392  
Response to Office action mailed Jan. 11, 2008  
Response filed April 18, 2008

when the units of machinery exhibit continuous operation without any signs of malfunction. ... *emerging malfunctions that may be anticipated and the service required thereby can be timed* as preventive maintenance. These actions counteract long shutdowns of production due to fault situations and allow servicing and spare parts installations to be carried out before actual malfunction has occurred. [Emphasis added.]

Paragraph [0030] is cited by the examiner for support for the proposition that “an automatic service process is started” but the Paragraph [0030] recites that the data may be accessed with the help of a www browser, clearly indicating data is provided to personnel, not that the step of claim 21 “*in a recognized emergency situation an automatic service process is started based on signals given by said monitoring systems...wherein the method functions statefully*” is suggested.

Paragraph [0029] is cited by the examiner for the proposition that the method of Maki is a method which “functions statefully”. However paragraph [0029] teaches “Data security is assured by identification of the IP addresses of the communicating computers and through the use of passwords and other authorization methods such as data transmission encryption” which does not describe a stateful firewall, i.e., programmed to distinguish legitimate packets for different types of connections by allowing only packets matching a known connection state through the firewall, nor the broader claimed concept of: a way of looking at data, and making decisions which is more than making decisions based only on administrator-defined rules.

With respect to claim 24, as argued above with respect to paragraph [0030], instructions issued to the production plant 20 are instructions only which are utilized by accessing the data using, for example, a web browser. Applicant claims not instructions for action, but taking action:

[0043] As a practical example.... If the quantity of broke exceeds the limit level, a message is generated in the SMAI unit and the message goes to the maintenance data system in the teleservice unit. Then a process support service is started, with which the process is set back to the operating point. All these

Applicant: Petteri Lannes et al.  
Application No.: 10/598,392  
Response to Office action mailed Jan. 11, 2008  
Response filed April 18, 2008

stages take place in real time and the messaging is brought about automatically in the system according to the invention. In state-of-the-art systems, broke has time to form over a long time in a corresponding situation, when people try to cope with the situation by making telephone calls or by using other such methods of communication....

With respect to claim 27 the examiner states “data measured earlier on the same or a similar object is utilized in the failure situation analysis (e.g., [0004])” the data utilized is not part of a stateful system.

Claim 33 claims a system for carrying out the process of claim 21. Again Maki does not disclose a stateful system for carrying out actions automatically. Paragraph [0030] instructions issued to the production plant 20 are instructions only, which are utilized by accessing the data using, for example, a web browser. Paragraph [0029] does not describe a stateful firewall, i.e., programmed to distinguish legitimate packets for different types of connections by allowing only packets matching a known connection state through the firewall, nor the broader claimed concept of: a way of looking at data, and making decisions, which is more than making decisions based only on administrator-defined rules.

Claims 23, 25, 28–30, and 32 were rejected over Maki in view of Hill. Hill is a system for monitoring printers and copiers, which reports remotely deviations from predetermined status conditions, and remotely adjusts the predetermined status conditions to be monitored.

Hill does not suggest a stateful system as described above nor the direct taking of action with respect to a papermaking machine, but only changing the parameters of the predetermined status conditions which does not correspond to applicant’s claimed stateful or statefully a way of looking at data, and making decisions, which is more than making decisions based only on administrator-defined rules (as in static analysis) but includes the context that has been established by prior information that has been processed by the information system and thus relies upon a unique configuration of information in a program or machine.

There is nothing in Hill that teaches the claimed step of claim 21 “in a recognized

Applicant: Petteri Lannes et al.  
Application No.: 10/598,392  
Response to Office action mailed Jan. 11, 2008  
Response filed April 18, 2008

emergency situation an automatic service process is started based on signals given by said monitoring systems” and specifically with respect to claim 28, the parameters adjusted by Hill are the parameters to be monitored, not the claimed “operating parameters of the machine” which by their adjustment, do not simply accept the problem, but solve the problem.

With respect to claim 30 the examiner confuses changing the allowed threshold value, so the machine is not considered to be out of an acceptable range, with the claimed step of changing the “operating parameters of the machine”. It is the difference between making the fault acceptable, and adjusting the machines so the fault does not occur or is tolerable.

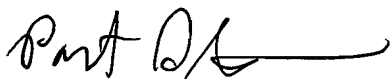
In conclusion, applicant claims a stateful method or system which is used to automatically affect the state of a papermaking machine to correct, or accommodate a fault with the machine. This claimed method and system differs from Maki, which is a monitoring system that provides information and instructions which can be acted on but does not act to change the machine. Hill is also a monitoring system, where the parameters to be monitored can be adjusted remotely, and does not teach adjusting the “operating parameters of the machine”, but only adjusting how the parameters are to be monitored.

Claims not specifically addressed add additional limitations which, in combination with the allowable base claim, further distinguish over the prior art.

Applicant believes that no new matter has been added by this amendment.

Applicant submits that the claims, as amended, are in condition for allowance.  
Favorable action thereon is respectfully solicited.

Respectfully submitted,



---

Patrick J. G. Stiennon, Reg. No. 34934  
Attorney for Applicant  
Stiennon & Stiennon  
P.O. Box 1667  
Madison, Wisconsin 53701-1667  
(608) 250-4870  
Amdt3.res

April 18, 2008 (10:25am)



**Check Point®**  
SOFTWARE TECHNOLOGIES LTD.

## **CHECK POINT SOFTWARE TECHNOLOGIES LTD. AWARDED PATENT FOR STATEFUL INSPECTION TECHNOLOGY**

**REDWOOD CITY, Calif., -- March 17, 1997** – Check Point Software Technologies Ltd. (NASDAQ: CHKPF), the market leader in enterprise security software, today announced that it has been awarded a patent from the United States Patent Office for its network security technology. The patent, U.S. Patent # 5,606,668, issued on February 25, 1997, covers, among other things, Check Point Software's implementation of "Stateful Inspection" technology for controlling network traffic, which includes a flexible, easily-alterable network security method for examining the information flow into and out of a network and making security decisions based on previously stored results.

"Stateful Inspection" is the technology upon which Check Point's award-winning Check Point™ FireWall-1™ enterprise security solution is based. To date, FireWall-1 is installed in over 16,000 locations worldwide.

"Since 1993, when Check Point Software invented our technique of examining network traffic and using the concept of state information, what we call "Stateful Inspection," we knew that this next-generation firewall technology would change the landscape of network security," said Gil Shwed, CEO of Check Point Software Technologies Ltd. "Many competitors have begun to emulate our Stateful Inspection technology, which validates the technology and has driven the creation of a widely-accepted new category within the network security market."

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. is the network security software market share leader and inventor of "Stateful Inspection" technology. According to a December 1996 report by the Yankee Group, the company's flagship product, Check Point FireWall-1, commanded 44% of the worldwide firewall market in the first half of 1996. FireWall-1 protects internal and external network communications for thousands of organizations of all sizes. Its products are sold worldwide through OEM partners, distributors, VARs, systems and network integrators and Internet Service Providers. The company has U.S. headquarters in Redwood City, California and international headquarters in Ramat-Gan, Israel. For product information, please call (800) 429-4391, e-mail [info@checkpoint.com](mailto:info@checkpoint.com) or visit Check Point Software at <http://www.checkpoint.com> .

###

1997 Check Point Software Technologies, Ltd. Check Point, the Check Point logo, Check Point FireWall-1, FireWall-1, FireWall-1 SecuRemote, FireWall-First! and INSPECT are trademarks of Check Point Software Technologies Ltd. All other product names mentioned herein are trademarks of their respective owners.

# Stateful firewall

From Wikipedia, the free encyclopedia

In computing, a **stateful firewall** (any firewall that performs **stateful packet inspection (SPI)** or **stateful inspection**) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU speed. Packet filters operate at the network layer (layer-3) and function more efficiently because they only look at the header part of a packet. However, pure packet filters have no concept of state as defined by computer science using the term finite state machine and are subject to spoofing attacks and other exploits.

## Contents

- 1 History
- 2 Description
- 3 Application-level filters
- 4 Pitfalls
- 5 See also
- 6 Notes

## History

Before the advent of stateful firewalls, a *stateless firewall*, a firewall that treats each network frame (or packet) in isolation, was normal. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet. Modern firewalls are connection-aware (or state-aware), affording network administrators finer-grained control of network traffic.

The classic example is the File Transfer Protocol, because by design it opens new connections to arbitrary ports. FTP, among other protocols, needs to be able to open connections to arbitrary high ports to function properly. Since a firewall has no way of knowing that the packet destined to the protected network, to some host's port 4970, is part of a legitimate FTP session, it will drop the packet. **Stateful firewalls** solve this problem by maintaining a table of open connections and intelligently associating new connection requests with existing legitimate connections.

## Description

A stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. The most CPU intensive checking is performed at the time of setup of the

connection. All packets after that (for that session) are processed rapidly because it is simple and fast to determine whether it belongs to an existing, pre-screened session. Once the session has ended, its entry in the state-table is discarded.

The stateful firewall depends on the famous three-way handshake of the TCP protocol. When a client initiates a new connection, it sends a packet with the SYN bit set in the packet header. All packets with the SYN bit set are considered by the firewall as NEW connections. If the service which the client has requested is available on the server, the service will reply to the SYN packet with a packet in which both the SYN and the ACK bit are set. The client will then respond with a packet in which only the ACK bit is set, and the connection will enter the ESTABLISHED state. Such a firewall will pass all outgoing packets through but will only allow incoming packets if they are part of an ESTABLISHED connection, ensuring that hackers cannot start unsolicited connections with the protected machine.

In order to prevent the state table from filling up, sessions will time out if no traffic has passed for a certain period. These stale connections are removed from the state table. Many applications therefore send keepalive messages periodically in order to stop a firewall from dropping the connection during periods of no user-activity, though some firewalls can be instructed to send these messages for applications. It is worth noting that the most common Denial of Service attack on the internet these days is the SYN flood, where a malicious user intentionally sends large amounts of SYN packets to the server in order to overflow its state table, thus blocking the server from accepting other connections.

Many stateful firewalls are able to track the state of flows in connectionless protocols, like UDP. Such sessions usually get the ESTABLISHED state immediately after the first packet is seen by the firewall. Sessions in connectionless protocols can only end by time-out.

By keeping track of the connection state, stateful firewalls provide added efficiency in terms of packet inspection. This is because for existing connections the firewall need only check the state table, instead of checking the packet against the firewall's rule set, which can be extensive. There is also an additional cost when the firewall's rule set is updated, which should cause the state table to be flushed. Also, the concept of deep packet inspection is unrelated to stateful firewalls / here the user data in the packet are inspected and as such it is application layer firewall /

## Application-level filters

However, packet filtering alone is not regarded as providing enough protection. In order to effectively block peer-to-peer-related network traffic, what is needed is a firewall that does *application filtering*, which can be regarded as an extension to stateful packet inspection. Stateful packet inspection can determine what type of protocol is being sent over each port, but application-level filters look at what a protocol is being used for. For example, an application-level filter might be able to tell the difference between HTTP traffic used to access a Web page and HTTP traffic used for file sharing, whereas a firewall that is only performing packet filtering would treat all HTTP traffic equally.

Application-layer firewalls differ from stateful packet-filtering and circuit-level gateways in several ways. Application-layer firewalls support multiple application proxies on a single firewall. The proxies sit between the client and server, passing data between the two endpoints. Suspicious data is dropped and the client and server never communicate directly with each other. Because application-level proxies are application-aware, the proxies can more easily handle complex protocols like H.323, which is used for videoconferencing and VoIP (voice over IP). Application proxies can be transparent to the client and



server, as no configuration is required on the client or the server; or can be nontransparent, letting the client and server address the proxy server directly. Transparency versus non transparency is a matter of implementation and address hiding, rather than about security.

## Pitfalls

Microsoft's latest operating system, Windows Vista, uses TCP window scaling for non-http (web) connections. So do Linux kernels from versions 2.6.8 on. This behavior is incompatible with some firewalls that use SPI (Stateful Packet Inspection) as found in routers like the Checkpoint NG R55, Cisco PIX IOS earlier than v6.3.1, NetApp Cache Appliances, SonicWall, D-Link DI-724U, Netgear WGR614, and Linksys WRT54GS. <sup>[1]</sup> This may be related to previous failures to work properly. Pre-released (beta) versions of Vista allegedly had more problems, including failed http (web) connections through SPI firewalls.<sup>[2]</sup>

## See also

- Network layer firewall
- Proxy server
- Cisco PIX
- FireWall-1
- Netfilter
- Iptables
- Kerio WinRoute Firewall
- CHX-I

## Notes

1. ^ Network connectivity may fail when you try to use Windows Vista behind a firewall device (<http://support.microsoft.com/kb/934430/en-us>).
2. ^ A painful Vista networking bug (<http://blogs.zdnet.com/Bott/?p=10>).

Retrieved from "[http://en.wikipedia.org/wiki/Stateful\\_firewall](http://en.wikipedia.org/wiki/Stateful_firewall)"

Categories: Computer network security

Hidden categories: All articles with unsourced statements | Articles with unsourced statements since October 2007 | Wikipedia articles needing clarification

- 
- This page was last modified on 14 March 2008, at 15:05.
  - All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.) Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.

# State (computer science)

From Wikipedia, the free encyclopedia

In computer science and automata theory, a **state** is a unique configuration of information in a program or machine. It is a concept that occasionally extends into some forms of systems programming such as lexers and parsers.

Whether the automaton in question is a finite state machine, a pushdown automaton or a full-fledged Turing machine, a state is a particular set of instructions which will be executed in response to the machine's input. The state can be thought of as analogous to a practical computer's main memory. The behavior of the system is a function of (a) the definition of the automaton, (b) the input and (c) the current state.

- **Compatible states** - are states in a state machine which do not conflict for any input values. Thus for every input, both states must have the same output, and both states must have the same successor (or unspecified successors) or both must not change. Compatible states are redundant if occurring in the same state machine.
  - **Equivalent states** are states in a state machine which, for every possible input sequence, the same output sequence will be produced - no matter which state is the initial state.
  - **Distinguishable states** are states in a state machine which have at least one input sequence which causes different output sequences - no matter which state is the initial state.
- 

In information processing, a **state** is the complete set of properties (for example, its energy level, etc. see state (physics)) transmitted by an object to an observer via one or more channels. Any change in the nature or quantity of such properties in a state is detected by an observer and thus a transmission of information occurs.

An information system or protocol that relies upon state is said to be *stateful*. One that does not is said to be *stateless*. For example, there are stateless firewalls and stateless servers, and HTTP is considered a stateless protocol. A character encoding such as ISO 2022 is said to be stateful if the interpretation of a particular code value depends on the code values that came before it.

## See also

- Clumping (computer science)
- State diagram
- program state
- finite state machine (FSM)

## References

- *Fundamentals of Digital Logic* by Brown and Vranesic


Retrieved from "[http://en.wikipedia.org/wiki/State\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/State_%28computer_science%29)"

Categories: Computational models | Cognition

- 
- This page was last modified on 23 March 2008, at 21:09.
  - All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)
- Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.

[internet.com](#)  
IT  
Developer  
News  
Compare Price Quotes - Contact Management Software  
Small Business  
ACT! 2008 Business Contact Manager  
Personal Tech  
Business Contact Management Solution  
Events  
Jobs

Virtual Pbx:  
Virtual PBX  
Virtual PBX From \$9.99 Per Month  
Virtual PBX

[internet.com](#) You are in the: Small Business Computing Channel 

Solutions  
» ECommerce-Guide | Small Business Computing | Webopedia | WinPlanet | Refer-It  
**Frost & Sullivan Report:** Learn how to meet key data archiving business challenges across your software environment & explore EMC's Integrated Content Archiving software platform.  
Login  
Register

[internet.com](#) **(Webopedia)** The #1 online encyclopedia dedicated to computer technology

## MENU

[Home](#)  
[Term of the Day](#)  
[New Terms](#)  
[Pronunciation](#)  
[New Links](#)  
[Quick Reference](#)  
[Did You Know?](#)  
[Categories](#)  
[Tech Support](#)  
[Technology Jobs](#)  
[About Us](#)  
[Link to Us](#)  
[Advertising](#)

[XML](#) [RSS](#)

**(Webopedia) Partners**

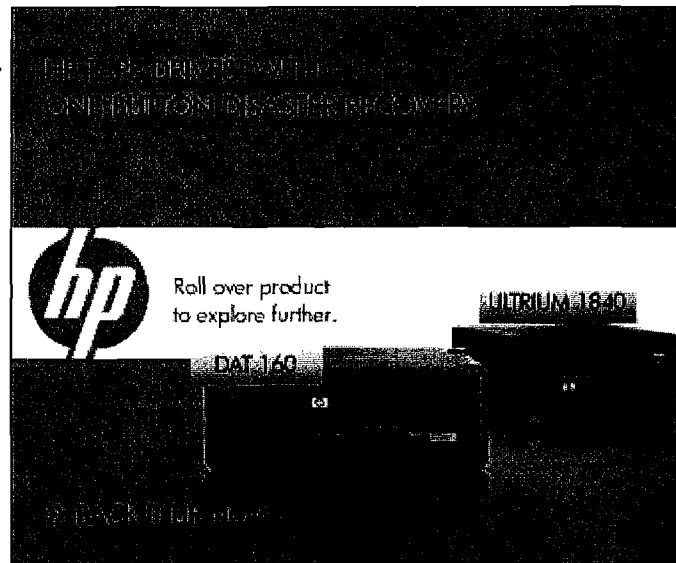
**Become a Marketplace Partner**

Find the right Business software now

# stateful inspection

Last modified: Monday, August 18, 2003

Also referred to as *dynamic packet filtering*. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful



Roll over product to explore further.

## Access Free Developer Tools

Download these IBM resources today!

**e-Kit: IBM Rational Systems Development Solution**

With systems teams under so much pressure to develop products faster, reduce production costs, and react to changing business needs quickly, communication and collaboration seem to get lost. Now, theres a way to improve product quality and communication.

**Webcast: Asset Reuse Strategies for Success--Innovate**

## TechnologyDirectory

Click for Technology &  
Business providers



World Class Web Hosting &  
more

inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall.

### Don't Duplicate!

Searching for, identifying, updating, using and deploying software assets can be a difficult challenge.

### eKit: Rational Build Forge Express

Access valuable resources to help you increase staff productivity, compress development cycles and deliver better software, fast.

### Download: IBM Data Studio v1.1

Effectively design, develop, deploy and manage your data, databases, and database applications throughout the data management life.

### eKit: Rational Asset Manager

Learn how to do more with your reusable assets, learn how Rational Asset Manager tracks and audits your assets in order to utilize them for reuse.

As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.

Check Point Software is credited with coining the term *stateful inspection* in the use of its FireWall-1 in 1993.

•**E-mail this definition to a colleague**•

## Related Categories

### Compare Prices:

Search here

go

shop.internet.com

Talk To Us...

Submit a URL  
Suggest a Term  
Report an Error

### Sponsored listings

**Property Records Search - \$39.95** - Access public record databases. Get detailed property information including owner info, property details, market value, area comps and more.

**Homeowners Insurance Quotes** - Provides homeowners insurance quotes for families and individuals. Works with multiple companies.

**Michigan Business Insurance From GLIGA** - Let us shop multiple companies for you and offer you 5 rates for your business insurance. One call quotes them all, or go to the website. Try us.

For internet.com pages about **stateful inspection** **CLICK HERE**. Also check out the following links!

### Security

## Related Terms

[application gateway](#)

[filter](#)

[firewall](#)

[IP spoofing](#)

[NAT](#)

[packet](#)

[packet filtering](#)

[port scanning](#)

[stateful](#)

\$8.50

Domains

internet.com

IT  
Developer  
Internet News  
Small Business  
Personal Technology  
International

Search internet.com  
Advertise  
Corporate Info  
Newsletters  
Tech Jobs  
E-mail Offers

internet commerce

Be a Commerce Partner  
Holiday Gift Ideas  
Condos For Sale

## LINKS

🚀 = Great Page!

### eSecurity Planet 🚀

A resource for daily information on e-security targeted to IT managers. The site provides users with information from a variety of sources, including experts at security product and services firms, and the consultants who follow the security industry.

## (Webopedia)

Give Us Your  
Feedback

Shopping  
stateful inspection Products  
Compare Products, Prices and  
Stores

Shop by Category: